CLAIMS

We Claim:

1. A method of ordering, paying for and delivering goods and services, comprising:

ordering and paying for a content by a user selected from a content provider;

transmitting a first service response value calculated by the user to the content provider;

calculating a second service response value by a network operator when the user requests the content from the network operator;

verifying, by the network operator contacting the content provider, that the first service response value matches the second service response value; and

transmitting the content to the user by the network operator when the first service response value matches the second service response value.

2. The method recited in claim 1, wherein the first service response value is calculated by the user based on a random number supplied by the content provider and a first secret key possessed by the user.

3. The method recited in claim 1, wherein the second service response value is calculated by the network operator based on the random number received

from the user and a second secret key possessed by the network operator and associated with the user.

4. The method recited in claim 2, wherein the first secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

5. The method recited in claim 3, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the network operator.

6. The method recited in claim 4, wherein the first service response value is calculated by an A3 algorithm module contained in the subscriber identification module of the mobile station based on the first secret key and the random number.

7. The method recited in claim 5, wherein the second service response value is calculated by an A3 algorithm module, contained in the authentication center of the telecom infrastructure, based on the second secret key, contained in the authentication center of the telecom infrastructure, and the random number.

8. The method recited in claim 6, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

9. The method recited in claim 7, wherein the content is encrypted by the network operator using a cipher key, calculated by an A8 algorithm module based on the random number and the second secret key, prior to transmitting the content to the user.

10. The method recited in claim 8, further comprising:

decrypting the content by the mobile station using an A8 algorithm module contained in the subscriber identification module of the mobile station to generate the cipher key based on the random number and the first secret key.

11. The method recited in claim 9, wherein the cipher key is used as a seed to a cryptographic protocol which transforms the cipher key into a stronger cipher key.

12. The method recited in claim 1, wherein the user pays the content provider for the content, using a credit card, debit card, or electronic transferral of funds.

13. A method of ordering, paying for and delivering goods and services, comprising:

ordering a content having a content ID by a user selected from a content provider;

transmitting a first service response value, a mobile network identifier, and a cipher key by the user to the content provider;

transmitting the first service response value, the mobile network identifier, and the random number to a network operator by the content provider;

calculating a second service response value and a cipher key by a network operator and determining if the first service response value matches the second service response value; and

transmitting the content to the user, when the first service response value matches second service response value, by the content provider.

14. The method recited in claim 13, wherein the first service response value is calculated by the user based on a random number supplied by the content provider and a first secret key contained in a subscriber identification module provided by the network operator and contained in a mobile station.

15. The method recited in claim 13, wherein the second service response value and a cipher key are calculated based on the random number, and a mobile network identifier, used to access a second secret key located in a authentication center of a telecom infrastructure, received from the content provider.

16. The method recited in claim 14, wherein the first secret key is not accessible directly by the user or the mobile station and the value of the secret key may not be discovered by the user, but is identical to the second secret key and both the first secret key and the second secret key are assigned when the user subscribes for a telecommunication service provided by the network operator.

17. The method recited in claim 16, wherein the first service response value is calculated by an A3 algorithm module contained in the subscriber identification module of the mobile station based on the first secret key and the random number.

18. The method recited in claim 15, wherein the second service response value is calculated by an A3 algorithm module, contained in the authentication center of the telecom infrastructure, based on the second secret key, contained in the authentication center of the telecom infrastructure, and the random number.

19. The method recited in claim 17, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

20. The method recited in claim 18, wherein the content is encrypted by the network operator using the cipher key, calculated by an A8 algorithm module based

on the random number and the second secret key, prior to transmitting the content to the user.

21. The method recited in claim 19, further comprising:

decrypting the content by the mobile station using an A8 algorithm module contained in the subscriber identification module of the mobile station to generate a cipher key based on the random number and the first secret key.

22. The method recited in claim 13, wherein the user is billed by the network operator for the content in a telephone bill.

23. The method recited in claim 13, further comprising:

hashing, by the user, a price of the content, the random number and a seller ID to create a hashed number;

computing, by the user, the first service response value based on the secret key and the hashed random number;

transmitting, by the user, the first service response value to the content provider;

transmitting, by the content provider, the random number, the seller ID the price of the content and the first service response to the network operator;

computing, by the network operator, the second service response value based on the secret key, the price transmitted by the content provider and the random number;

verifying, by the network operator that the first service response value matches the second service response value; and

billing the user, by the network operator, the price when the first service response value matches the second service response value in a telephone bill.

24. The method recited in claim 20, wherein the cipher key is used as a seed to a cryptographic protocol which transforms the cipher key into a stronger cipher key.

25. A method of ordering, paying for and delivering goods and services, comprising:

ordering a content from a network operator, having a content ID selected by a user;

transmitting a first service response value calculated by the user to the network operator;

calculating a second service response value and a cipher key by a network operator and determining if the first service response value matches the second service response value;

transmitting the content ID, and a cipher key to the content provider; and

transmitting the content to the user by the content provider when requested by the user.

26. The method recited in claim 25, wherein the first service response value is calculated by the user based on a random number supplied by the network operator and a first secret key possessed by the user.

27. The method recited in claim 25, wherein the second service response value is calculated by the network operator based on the random number and a second secret key possessed by the network operator and associated with the user.

28. The method recited in claim 26, wherein the first secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

29. The method recited in claim 27, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the network operator.

30. The method recited in claim 28, wherein the first service response value is calculated by an A3 algorithm module contained in the subscriber identification module of the mobile station based on the first secret key and the random number.

31. The method recited in claim 29, wherein and the second service response value is calculated by a A3 algorithm module, contained in the authentication center of the telecom infrastructure based on the second secret key, contained in the authentication center of the telecom infrastructure, and the random number.

32. The method recited in claim 30, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

33. The method recited in claim 31, wherein the content is encrypted by the content provider using a cipher key, calculated by an A8 algorithm module based on the random number and the second secret key and supplied by the network operator, prior to transmitting the content to the user.

34. The method recited in claim 32, further comprising:

decrypting the content received by from the content provider by the mobile station using an A8 algorithm module contained in the subscriber identification module of the mobile station to generate a cipher key based on the random number and the first secret key.

35. The method recited in claim 33, wherein the cipher key is used as a seed to a cryptographic protocol which transforms the cipher key into a stronger cipher key.

36. The method recited in claim 25, wherein the user is billed by the network operator for the content in a telephone bill.

37. A method of ordering, paying for and delivering goods and services, comprising:

ordering a content, having a content ID, by a user selected from a network operator;

transmitting a first service response value calculated by the user to the network operator;

calculating a second service response value and a cipher key by a network operator and determining if the first service response value matches the second service response value; and

transmitting the content to the user by the network operator when requested by the user.

38. The method recited in claim 37, wherein the first service response value is calculated by the user based on a random number supplied by the network operator and a first secret key possessed by the user.

39. The method recited in claim 37, wherein the second service response value is calculated by the network operator based on the random number and a second secret key possessed by the network operator and associated with the user.

40. The method recited in claim 38, wherein the first secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

41. The method recited in claim 39, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the network operator.

42. The method recited in claim 40, wherein the first service response value is calculated by an A3 algorithm module contained in the subscriber identification module of the mobile station based on the first secret key and the random number.

43. The method recited in claim 41, wherein the second service response value is calculated by an A3 algorithm module, contained in the authentication center of the telecom infrastructure, based on the second secret key, contained in the authentication center of the telecom infrastructure, and the random number.

44. The method recited in claim 42, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

45. The method recited in claim 43, wherein the content is encrypted by the network operator using a cipher key, calculated by an A8 algorithm module based on the random number and the second secret key and supplied by the network operator, prior to transmitting the content to the user.

46. The method recited in claim 44, further comprising:

decrypting the content received by from the network operator by the mobile station using an A8 algorithm module contained in the subscriber identification module of the mobile station to generate a cipher key based on the random number and the first secret key.

47. The method recited in claim 45, wherein the cipher key is used as a seed to a cryptographic protocol which transforms the cipher key into a stronger cipher key.

48. The method recited in claim 37, wherein the user is billed by the network operator for the content in a telephone bill.

49. A method of ordering, paying for and delivering goods and services, comprising:

ordering and paying for a plurality of contents by a user selected from a content provider;

transmitting a plurality of first service response values calculated by the user to the content provider;

calculating a plurality of second service response values by a network operator when the user requests the content from the network operator;

verifying, by the network operator contacting the content provider, that a one of the plurality of first service response values matches a one of the plurality of second service response values; and

transmitting a content of the plurality of contents to the user by the network operator when the one of the plurality of first service response values matches the one of the plurality of second service response values.

50. The method recited in claim 49, wherein the plurality of first service response values are calculated by the user based on a plurality of random numbers supplied by the content provider and a first secret key possessed by the user.

51. The method recited in claim 49, wherein the plurality of second service response values are calculated by the network operator based on the plurality of random numbers received from the user and a second secret key possessed by the network operator and associated with the user.

52. The method recited in claim 50, wherein the first secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key.

53. The method recited in claim 51, wherein the second secret key is stored in an authentication center of a telecom infrastructure operated by the network operator and the first secret key and the second secret key are identical and assigned when the user subscribes for a telecommunication service provided by the network operator.

54. The method recited in claim 52, wherein the plurality of first service response values are calculated by an A3 algorithm module contained in the subscriber identification module of the mobile station based on the first secret key and the plurality of random numbers.

55. The method recited in claim 53, wherein and the plurality of second service response values are calculated by an A3 algorithm module, contained in the authentication center of the telecom infrastructure based on the second secret key, contained in the authentication center of the telecom infrastructure, and the plurality of random numbers.

56. The method recited in claim 54, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

57. The method recited in claim 55, wherein the content of the plurality of contents is encrypted by the network operator using a cipher key, calculated by an A8 algorithm module based on a random number of the plurality of random numbers and the second secret key, prior to transmitting the content of the plurality of contents to the user.

58. The method recited in claim 56, further comprising:

decrypting the content of the plurality of contents by the mobile station using an A8 algorithm module contained in the subscriber identification module of the mobile station to generate a cipher key based on the random number of the plurality of random numbers and the first secret key.

59. The method recited in claim 57, wherein the cipher key is used as a seed to a cryptographic protocol which transforms the cipher key into a stronger cipher key.

60. The method recited in claim 49, wherein the user pays the content provider for the plurality of contents, using a credit card, debit card, or electronic transferral of funds.

61. A computer program executable by a processor and embodied on a computer readable medium to pay for and deliver goods and services, comprising:

an A3 algorithm module code segment to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a content provider after a user selects a content having a content ID to purchase; and

a business model A module code segment to enable a user to select the content having the content ID from the content provider and receive the random number from the content provider, transmit the service response value to the content provider computed by the A3 algorithm module code segment, transmit the content ID, and the random number to a network operator and receive the content from the network operator based on verification of the content ID, the random number, and the service response value by the content provider.

62. The computer program recited in claim 61, further comprising:

an A8 algorithm module code segment to compute a cipher key based on the random number and the secret key and used to encrypt the content.

63. The computer program recited in claim 62, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

64. The computer program recited in claim 63, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

65. The computer program recited in claim 64, wherein the user pays the content provider for the content, using a credit card, debit card, or electronic transferral of funds.

66. A computer program executable by a processor and embodied on a computer readable medium to pay for and deliver goods and services, comprising:

an A3 algorithm module code segment to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a content provider after a user selects a content having a content ID to purchase; and

a business model B module code segment to enable a user to select the content having the content ID from the content provider and receive the random

number from the content provider, transmits a mobile network identifier and the service response value to the content provider computed by the A3 algorithm module code segment, transmit the content ID, and the random number to a network operator and receive the content from the content provider based on verification of the content ID, the random number, and the service response value by the content provider and the network operator.

67. The computer program recited in claim 66, further comprising:

an A8 algorithm module code segment to compute a cipher key based on the random number and the secret key and used to encrypt the content.

68. The computer program recited in claim 67, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

69. The computer program recited in claim 68, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

70. The computer program recited in claim 66, wherein the business model B module code segment bills the user for the content in a telephone bill network operator.

71. The computer program recited in claim 66, further comprising:

a one-way hash function code segment contained in the mobile station and the network operator to generate a hashed number based on the random number, a seller ID and a price for the content; and

the A3 algorithm module code segment contained in the mobile station and the network operator to generate the first service response value calculated by the mobile station based on the secret key and hashed number and the second service response calculated by network operator based on the secret key and a seller ID, random number and price transmitted by the content provider to the network provider, wherein the user is billed for the price in a telephone bill when the first service response value matches the second service response value.

72. The computer program recited in claim 71, further comprising:

a cryptographic protocol which uses the cipher key as a seed to transform the cipher key into a stronger cipher key.

73. A computer program executable by a processor and embodied on a computer readable medium to pay for and deliver goods and services, comprising:

an A3 algorithm module code segment to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a network operator after a user selects a content having a content ID to purchase; and

a business model C module code segment to enable a user to select the content having the content ID from the network operator and receive the random number from the network operator, transmits the service response value to the network operator computed by the A3 algorithm module code segment, transmit the content ID, and the random number to a content provider and receive the content from the content provider based on verification of the content ID, the random number, and the service response value having been sent by the network provider.

74. The computer program recited in claim 73, further comprising:

an A8 algorithm module code segment to compute a cipher key based on the random number and the secret key and used to encrypt the content.

75. The computer program recited in claim 74, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

76. The computer program recited in claim 75, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

77. The computer program recited in claim 73, wherein the business model C module code segment bills the user for the content in a telephone bill from the network operator.

78. A computer program executable by a processor and embodied on a computer readable medium to pay for and deliver goods and services, comprising:

an A3 algorithm module code segment to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a network operator after a user selects a content having a content ID to purchase; and

a business model D module code segment to enable a user to select the content having the content ID from the network operator and receive the random number from the network operator, transmits the service response value to the network operator computed by the A3 algorithm module code segment, transmit the content based on verification of the service response value having been sent by the user.

79. The computer program recited in claim 78, further comprising:

an A8 algorithm module code segment to compute a cipher key based on the random number and the secret key and used to encrypt the content.

80. The computer program recited in claim 79, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

81. The computer program recited in claim 80, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

82. The computer program recited in claim 78, wherein the business model D module code segment bills the user for the content in a telephone bill from the network operator.

83. A computer program executable by a processor and embodied on a computer readable medium to pay for and deliver goods and services, comprising:

an A3 algorithm module code segment to compute a plurality of service response values based a secret key, possessed by a user and a network operator,

and on a plurality of random numbers provided by a content provider after a user selects a plurality of contents having a plurality of content IDs to purchase; and

a business model E module code segment to enable a user to select the plurality of contents having the plurality of content IDs from the content provider and receive the plurality of random numbers from the content provider, transmit the plurality of service response values to the content provider computed by the A3 algorithm module code segment, transmit one content ID of the plurality of content IDs, and one random number of the plurality of random numbers to a network operator and receive the content from the network operator based on verification of the one content ID, the one random number, and the one service response value by the content provider.

84. The computer program recited in claim 83, further comprising:

an A8 algorithm module code segment to compute a cipher key based on the one random number and the secret key and used to encrypt the one content.

85. The computer program recited in claim 84, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

86. The computer program recited in claim 85, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

87. The computer program recited in claim 83, wherein the user pays the content provider for the content, using a credit card, debit card, or electronic transferal of funds.

88. A system to pay for and deliver goods and services, comprising:

an A3 algorithm module to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a content provider after a user selects a content having a content ID to purchase; and

a business model A module to enable a user to select the content having the content ID from the content provider and receive the random number from the content provider, transmit the service response value to the content provider computed by the A3 algorithm module, transmit the content ID, and the random number to a network operator and receive the content from the network operator based on verification of the content ID, the random number, and the service response value by the content provider.

89. The system recited in claim 88, further comprising:

an A8 algorithm module to compute a cipher key based on the random number and the secret key and used to encrypt the content.

90. The system recited in claim 89, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

91. The system recited in claim 90, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

92. The system recited in claim 88, wherein the user pays the content provider for the content, using a credit card, debit card, or electronic transferral of funds.

93. A system to pay for and deliver goods and services, comprising:

an A3 algorithm module to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number

provided by a content provider after a user selects a content having a content ID to purchase; and

a business model B module to enable a user to select the content having the content ID from the content provider and receive the random number from the content provider, transmits a mobile network identifier and the service response value to the content provider computed by the A3 algorithm module, transmit the content ID, and the random number to a network operator and receive the content from the content provider based on verification of the content ID, the random number, and the service response value by the content provider and the network operator.

94. The system recited in claim 93, further comprising:

an A8 algorithm module to compute a cipher key based on the random number and the secret key and used to encrypt the content.

95. The system recited in claim 94, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

96. The system recited in claim 95, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

97. The system recited in claim 93, wherein the business model B module bills the user for the content in a telephone bill network operator.

98. The system recited in claim 93, further comprising:

a one-way hash function contained in the mobile station and the network operator to generate a hashed number based on the random number, a seller ID and a price for the content; and

the A3 algorithm module contained in the mobile station and the network operator to generate the first service response value calculated by the mobile station based on the secret key and hashed number and the second service response calculated by network operator based on the secret key and a seller ID, random number and price transmitted by the content provider to the network operator, wherein the user is billed for the price in a telephone bill when the first service response value matches the second service response value.

99. The system recited in claim 98, further comprising:

a cryptographic protocol which uses the cipher key as a seed to transform the cipher key into a stronger cipher key.

100. A system to pay for and deliver goods and services, comprising:

an A3 algorithm module to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a network operator after a user selects a content having a content ID to purchase; and

a business model C module to enable a user to select the content having the content ID from the network operator and receive the random number from the network operator, transmits the service response value to the network operator computed by the A3 algorithm module, transmit the content ID, and the random number to a content provider and receive the content from the content provider based on verification of the content ID, the random number, and the service response value having been sent by the network provider.

101. The system recited in claim 100, further comprising:

an A8 algorithm module to compute a cipher key based on the random number and the secret key and used to encrypt the content.

102. The system recited in claim 101, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

103. The system recited in claim 102, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

104. The system recited in claim 103, wherein the business model C module bills the user for the content in a telephone bill from the network operator.

105. A system to pay for and deliver goods and services, comprising:

an A3 algorithm module to compute a service response value based a secret key, possessed by a user and a network operator, and on a random number provided by a network operator after a user selects a content having a content ID to purchase; and

a business model D module to enable a user to select the content having the content ID from the network operator and receive the random number from the network operator, transmits the service response value to the network operator computed by the A3 algorithm module, transmit the content based on verification of the service response value having been sent by the user.

106. The system recited in claim 105, further comprising:

an A8 algorithm module to compute a cipher key based on the random number and the secret key and used to encrypt the content.

107. The system recited in claim 106, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in a authentication center of a telecom infrastructure operated by the network operator.

108. The system recited in claim 107, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

109. The system recited in claim 105, wherein the business model D module bills the user for the content in a telephone bill from the network operator.

110. A system to pay for and deliver goods and services, comprising:

an A3 algorithm module to compute a plurality of service response values based a secret key, possessed by a user and a network operator, and on a plurality of random numbers provided by a content provider after a user selects a plurality of contents having a plurality of content IDs to purchase; and

a business model E module to enable a user to select the plurality of contents having the plurality of content IDs from the content provider and receive the plurality of random numbers from the content provider, transmit the plurality of service response values to the content provider computed by the A3 algorithm module,

transmit one content ID of the plurality of content IDs, and one random number of the plurality of random numbers to a network operator and receive the content from the network operator based on verification of the one content ID, the one random number, and the one service response value by the content provider.

111. The system recited in claim 110, further comprising:

an A8 algorithm module to compute a cipher key based on the one random number and the secret key and used to encrypt the one content.

112. The system recited in claim 111, wherein the secret key is contained in a subscriber identification module provided by the network operator and contained in the mobile station in such a manner that the user and the mobile station may not discover the value of the secret key and the secret key is also stored in an authentication center of a telecom infrastructure operated by the network operator.

113. The system recited in claim 112, wherein the mobile station is a cellular phone with GSM authentication capability connected to a processor based system, or a WAP-capable cellular phone with GSM authentication capability, or a HTML capable cellular phone with GSM authentication capability.

114. The system recited in claim 108, wherein the user pays the content provider for the content, using a credit card, debit card, or electronic transferral of funds.